The Effect of Behavioral Tracking Practices on Consumers' Shopping Evaluations and Repurchase Intention toward Trusted Online Retailers

1. Introduction

As the e-commerce sector has experienced double-digit rate increases annually in the United States (comScore.com, 2012), privacy issues pertaining to consumer data continue to be of serious concern. In a national online privacy survey, ninety percent of Americans indicated they are worried about their privacy online (TRUSTe, 2012). Regardless of users' concerns, the Internet has become an essential part of life for many people. The apparel/accessories category, for example, is currently the second largest e-commerce product category (behind computer product category) and is responsible for nearly 14 billion US dollars in web sales (Internet Retailer, 2009). Online shoppers can easily shop with online retailers via devices such as personal computers, smart phones, or tablets (e.g., the iPad) by connecting with retailers' online storefronts, mobile apps or social networks. A recent *Time Magazine* article (Stein, 2011) reported that with a name and email address, a data mining company can easily compile a vast amount of personal data about individual consumers, including online/offline shopping history, social media preferences, demographic information, and data from any consumer loyalty programs that the consumer has joined. Whereas consumers may initially share personal information with online retailers to either complete purchase transactions or participate in a consumer loyalty programs, retailers may also use, sell, or share such information for secondary marketing purposes. Current U.S. legislation does not give consumers the right to refuse to be tracked online or to refuse targeted advertising (FTC, 2009). However, Turow, King, Hoofnagle, Bleakley, and Hennessy (2009) found that most Americans did not know whether a company had the right to sell or share their information and "mistakenly believe that current government laws restrict companies from selling wide-ranging data about them" (p. 4).

A number of online and offline retailers have been criticized or sued for using consumer personal data to exercise price discrimination (CNN, 2005), retargeting ads (New York Times, 2010), and disrespecting consumers' choice of privacy setting (Internet Retailer, 2011). Although online retailers may use consumer data to tailor their offerings and promotion strategies to individual consumers, this data may also be used outside of the original shopping context. For example, it is possible that consumers' apparel/accessory shopping history such as sizes and brands shopped may be used for insurance disqualification/rate setting. It is also possible that demographic information such as residence address, age, or income level may be used for evaluating consumers' ability to pay higher prices, or setting unfavorable mortgage rates or terms.

The purpose of this study was to examine the effect of behavioral tracking on consumers' responses in the trusted online shopping context. The term *behavioral tracking* refers to tracking

that has not been expressly authorized by the consumer after the consumer has been given adequate notice of the information privacy practices of the company doing the tracking. Specifically, the present study examined how consumers' evaluations of online shopping experiences (perceived benefit, risk, and unfairness) and repurchase intention were influenced when exposed to information about behavioral tracking practices.

Information privacy issues have become a central topic in e-commerce research across many disciplines (Smith, Dinev & Xu, 2011). It has been observed that the advanced online behavioral tracking methods have raised concerns about consumers' information privacy (Turow, King, Hoofnagle, Bleakley, & Hennessy, 2009), especially focusing on the expanding roles of third-party businesses (King, 2011; Mayer, 2011). Researchers have conducted studies about consumers' cognitive knowledge of online information privacy (Park, Campbell, & Kwak, 2012), consumers' decisions to disclose personal information to unfamiliar online vendors (Li, Sarathy, & Xu, 2011), and their privacy concerns about personalization marketing (Chellappa & Sin, 2005). In the online environment, the concept of personal-identifiable information (PII) has diminished relevance as it becomes easier to associate an individual with a digital device. A Federal Trade Commission (FTC, 2012) report acknowledges "consumers' objections to being tracked, regardless of whether the tracker explicitly learns a consumer name, and the potential for harm, such as discriminatory pricing based on online browsing history, even without the use of PII" (p.18). When knowledge about behavioral targeting is made available to consumers, it is expected that behavioral tracking would raise ethical flags about damage that can be done to consumers' privacy and consequently, raise their concern about that damage. The results of this research may help increase retailers' awareness regarding how behavioral targeting practices influence consumers' future repurchase intention on their trusted websites.

2. Behavioral Tracking and Consumers' Personal Information

Online behavioral targeting is a marketing practice of collecting and compiling a record of individual consumers' online activities, interests, preferences, and/or communications over time and across websites in order to deliver personalized advertising (FTC, 2009). Many online retailers allow third-party advertisers to put small text files called "cookies" into the Internet browser programs on consumers' computer drives (Miyazaki, 2008). When installed in a consumer's computer drive, cookies allow online marketers and third-party advertisers to track consumers' browsing behaviors across websites, enabling these advertisers to provide personalized advertising based upon their browsing behaviors (Cranor, 1999; FTC, 2009).

Providing personalized advertising is one of the hottest trends in online retailing (Turban, King, Lee, Liang & Turban, 2010). In conducting personalized marketing, consumers' personal data (e.g. name, geographic location, income, family size, brand preference, shopping history) is

a crucial asset for marketers. Thus, the collection of consumer data is an almost universal practice of commercial websites.

3. Theoretical Framework and Hypotheses Development

One of the most classic models in the field of environmental psychology is the Stimulus-Organism-Response (SOR) model (Mehrabian & Russell, 1974), which depicts how the recognition of situational variables (stimulus) can influence consumers' internal organism (such as emotions, attitudes) and external responses (approach/avoidance behaviors). The present study applies the Stimulus-Organism-Response (SOR) model to investigate the effect of behavioral practices scenarios (stimulus) on consumers' evaluations of their online shopping experiences (internal organism) and repurchase intention toward online retailers (external responses).

3.1 Stimulus-Behavioral Tracking Practices

Milne and Rohm (2000) argued that consumer privacy exists only when consumers are aware of their information being collected and are able to remove their names from undesirable lists (exercise control) if they wish. When businesses collect, use, or share consumers' personal information, they should follow five core Fair Information Practice Principles: notice/awareness, choice/consent, access/participation, integrity/security and enforcement/redress (FTC, 2007). In the present study, consumers' information privacy refers to consumers' ability to control who, how, and to what extent their personal information is transmitted to others (Goodwin, 1991; Lanier & Saini, 2008; Phelps, Nowak, & Ferrell, 2000).

In the present study, the designed scenarios (see Appendix A) served as stimuli to evoke consumer awareness of online retailers' behavioral tracking practices, hence to internally evaluate if the social exchange relationship is fair to them. Stimuli included both the number of third party cookies placed in the consumer's computer while shopping their trusted site and the level to which the retailer disseminated their information.

3.2 Organism-perceived benefit, risk, and fairness

Social Contract (SC) theory has been suggested to examine ethical issues in marketing (Dunfee, Smith & Ross, 1999). The hypothetical social contract in a customer-firm relationship is that the firm offers advantages to society (its customers and employees) in exchange to exist and thrive (Dunfee, Smith & Ross, 1999). Applying the Social Contract framework, researchers have found that consumers performed cost-benefit ("tradeoff") evaluations when they engaged in online information exchange (Culnan & Bies, 2003; Malhotra, Kim, & Agarwal, 2004). This tradeoff evaluation has been studied offline as a "privacy calculus," which measures the usage of personal information (benefit) against the potential negative consequences (cost) of its dissemination (Milne & Gordon, 1993). In the online retailing context, the willingness of consumers to share their personal information during online shopping involves evaluating the benefits and risks of online behavioral tracking practices and the release of personal information,

hence to form an evaluation of unfairness of providing personal information with the trusted online retailers.

In this study, the perceived benefits were defined as the pleasure of seeing personalized advertisements while using social networks, while reading news from a news website or while using the online email services. The items were adopted from prior research (Yu & Cude, 2009). Consumers are aided in their shopping experience by accessibility of knowledge of retail choices that are particularly relevant to their needs or preferences. Third-party cookies enable online third-party advertisers like Google to more precisely follow web-surfing behavior across affiliated sites, like Google Search (search engine), You Tube (publisher), and Gmail (email service) and to provide personalized advertisements.

Meanwhile, consumers' perceived risk of behavioral tracking reflects their concerns about potential privacy invasion associated with retailers' online information practices. Prior research suggests information privacy concerns are raised when consumers feel uninformed by marketers about who are collecting their personal information, how their information is collected, and for what purpose their information is used (Lanier & Saini, 2008; Nowak & Phelps, 1995). Widely-used behavioral tracking, where marketers track consumers' online use and collect information about consumers without their awareness or consent, is considered by many researchers to be a breach of an implied social contract to protect consumers' information privacy that may harm consumer trust and patronage (Miyazaki, 2008; Poddar, Mosteller, & Ellen, 2009). Consumers' perceived risk about their information privacy may be heightened when they feel they do not have the ability to control with, how, and to what extent their personal information is transmitted to others. In this study, we hypothesize that when a consumer is informed that he/she has been subject to behavioral tracking, he/she may feel uninformed and to have lost control of their personal information and this may increase his/her perceived risk of interacting with the retailer online. Thus, the following hypotheses were developed:

H1: The number of third-party cookies will have a positive relationship with perceived risk of shopping on the websites.

H2: The number of third-party cookies will have a negative relationship with perceived benefit about personalized ads.

H3: The level of disseminating consumer information has a positive relationship with perceived risk of shopping on the websites.

H4: The level of disseminating consumer information has a negative relationship with perceived benefit about personalized ads.

Fairness is viewed as a fundamental concern in social exchange relationship (Huang, 2001). A consumer's personal information can be seen as a valuable asset for exchange (Culnan & Bies, 2003). As a result, in the context of online shopping, it is expected that perception of risk about

losing control over one's personal information will have a negative relationship with perceived fairness of transactions. However, previous researches have shown that consumers disclose their personal information to obtain "free" information, personalized content (Pastore, 1999), or some other form of "fair" exchange (Culnan & Bies, 2003). As the result, it is expected that the perceived benefit of personalized advertising provided by behavioral tracking practices will have a positive relationship with perceived fairness of transactions. Thus, the following hypotheses were developed:

H5: Consumers' perceived risk of shopping on the websites has a positive relationship with (a) perceived unfairness.

H6: Consumers' perceived benefit about personalized ads has a negative relationship with perceived unfairness.

3.3 Response-Repurchase Intention

Repurchase intention can be viewed as a behavioral component of consumer attitude in online shopping field (Hawkins, Mothersbaugh, & Best, 2007). The cognition of perceived unfairness towards the online shopping experience may reduce consumers' willingness for future repurchase intention (Huang, 2001). It is expected that consumers' perception of unfairness of shopping on the websites will have a negative relationship toward consumers' repurchase intention. Applying the SOR model, it is expected that consumers' perceived risk, benefit, and unfairness about shopping with the online retailers will mediate the effect of behavioral tracking practices on consumers' behavioral responses (repurchase intention). Thus, the following hypotheses were developed:

H7: Consumers' repurchase intention has a negative relationship with perceived unfairness.

H8: Perceived risk, benefit and unfairness mediate the effect of behavioral tracking practices on consumers' repurchase intention.

4. Method

A between-subject experimental design was employed to test the research model. Four versions of a questionnaire were developed on a commercial online survey website in which the surveys were randomly distributed to respondents and data were collected. The questionnaires included five major sections. In the first section, every respondent was asked to identify a website at which they frequently shop (later to be indicated within scenarios as MyFavoriteStore.com). Questions asked included which product category best described their shopping choices at the website, how frequently they patronized the website, and their commitment toward website. Consumer commitment is an attitude which involves one's beliefs and acceptance of the origination's goals and values, expression of authentic interest in the company's interests, expenditure of considerable effort on its behalf, and desire to remain a consumer (Huang, 2001). The 5-item scale adopted from Ingram, Skinner and Taylor (2005)

included questions such as "I am a loyal patron of this website", "I believe that my values are in line with the values of the website", "I spend a lot of time on this website searching for or purchasing products" and "I introduce/recommend this website to my friends." These items were measured with 7-point Likert scales anchored with "1 Strongly Disagree" and "7 Strongly Agree." This section was designed to verify that the respondent had established a trust relationship with the identified online retailer. The second section included questions of cookies usage in websites (Table 1). This section was designed to understand respondents' knowledge of cookies and to provide knowledge of the cookies usage before they proceeded to next section. In the third section, subjects were then exposed to one of the three behavioral tracking scenarios presented below (except the control group). The fourth section included questions measuring perceived benefit, risk, unfairness, and repurchase intention regarding shopping on the identified website. All questions in sections two and four were measured with 7-point Likert scales anchored with "1 Strongly Disagree" and "7 Strongly Agree." The last section included questions asking for demographic information such as gender, age, class standing, and ethnicity. All measurements of latent constructs are reported in Table 2.

4.1 Scenario Designs

We developed three behavioral tracking scenarios to evoke different levels of perceived risk. Two factors were manipulated: (1) the number of third-party cookies identified on their favorite website (0 or 14) and (2) the level of disseminating consumers' personal information (internally share with corporate family versus externally share with other third-party companies). We skipped one condition (14 third-party cookies and share consumer data only with the corporate family), because the scenario may be considered deceptive as these two factors conflict to each other regarding the range of data sharing. In the scenario, we told respondents first to imagine that one of their friends told them to use a software program to identify whether third-party cookies were placed in their computer drives when they visit a website, and then after using the software, they learned that their favorite website allowed the manipulated number (0 or 14) of third-party cookies installed in their computer hard drives. Following the third-party cookie identification information, the scenario then presented an excerpt of a privacy policy adapted from a major online retailer's for manipulation purposes. The excerpt described how, why and with whom the website shared their personal and website navigation information: (1) internally within the corporate family (also called affiliates—companies under common ownership) or also (2) externally with companies outside of their corporate family. In the latter case, other merchants could use the information to send offers about their products and services. The control group's questionnaire included all sections except the behavioral tracking scenario. In the scenario, we defined personal information as name, postal and email address, product preference and purchase history; the website navigation information included IP address, the site that the

consumer navigated from, and the site that consumer navigates to when they leave the website. We also told respondents that their personal information may be connected with their navigation information (see Appendix A).

4.2 Sample

A purposive convenience sample was used in the study. Respondents were recruited from a northwestern US university either via an electronic mailing list system used at the university or through selected course instructors in the Colleges of Business and Public Health and Human Sciences. In some cases, respondents received extra credit for participation. College students were chosen because they not only represent a vulnerable and significant Internet user group, but they are also an important cohort, Generation Y, to online retailers (National Retail Federation, 2007). They have the highest Internet usage of any other cohort and their online buying and purchasing behavior is representative of technology savvy users (Fox & Madden, 2005; LaRose & Rifon, 2007).

4.3 Manipulation check

In order to ensure the manipulations were effective, the mean value of perceived risk of each condition was tested. The results of ANOVA shows that there is a significant difference of perceived risk between conditions [F (3, 420) = 33.58, $p<.001$]. The scenario in which retailers are found to allow 14 third-party cookies and to share consumer data both internally and externally evoked the highest perceived risk (n=116, mean=4.72), followed by those which allow no third-party cookies identified but shared data both internally and externally (n=147, mean=4.58), and those which allow no third-party cookies and only shared data internally (n=91, mean=4.21). The respondents in the control group have the lowest perceived risk scores (n=80, mean=2.85). These results provide support for the effectiveness of the manipulation.

5. Results

5.1 Characteristics of Respondents

A total of 417 college students aged 18 to 35 years completed the survey in this study. Most respondents were female (71.2%) and ranged from 18 to 25 years in age (93.8%). Of the total responses, about 90% of respondents reported that they shopped at least once a month on the website which they identified and about 86% of them reported that they had made purchases on the websites. In order to ensure that respondents in different conditions (control and three manipulated conditions) had similar level of trust relationship with their identified online retailers, a one-way between subjects ANOVA was conducted to compare the mean values of commitment towards online retailers among different conditions. The results of ANOVA showed that there was no significant difference of commitment toward online retailers among the four conditions [F (3, 428) = .51, *n.s.*]. The means of commitment toward online retailers in four

conditions were all above 4 (ranged from 4.71 to 4.89) in a 7-point Likert scale, which suggested that respondents have developed a certain level of trusted relationship with the online retailers.

For respondents' online shopping preferences, "clothing/shoes/accessories" was the highest reported product category (70.2%), followed by books/magazines category (22.9%). Under the category of "Clothing/shoes/accessories", a total of 67 websites were reported. Nordstrom.com (17.7%), Forever 21.com (13.4%) and Victoria's Secret.com (9.9%) were the top three most frequently visited websites. With regards to respondents' behavior and knowledge about "cookies" used on the Internet, 72.7 % of respondents reported that they had deleted "cookies" from their hard drive, while only 37% of respondents reported that they knew that some websites allow other third-party companies to place cookies into visiting customers' hard drives in order to track web shopping behaviors. How respondents' knowledge and behavior about cookies may have influence on this research results are discussed in Discussion section. More details of respondents' characteristics are provided in Table 1.

Table 1 Characteristics of Respondents (N=417)

Characteristics		Percentage
Gender	Male	27.6
	Female	71.2
	Missing	1.2
Age	18-25	93.8
	26-35	6.2
Class Standing	1. Freshman	15.2
	2. Sophomore	14.3
	3. Junior	30.1
	4. Senior	34.4
	5. Graduate	6.0
Ethnic Group	1. White, non-Hispanic	76.3
	2. Asian	11.1
	3. Hispanic/Latino	6.0
	7. Other	6.4
Shopping Category (multiple choice)	1. Clothing/shoes/accessories	70.2
	2. Books/magazines	22.9
	3. Entertainment (CD, videos, concert tickets)	14.3
	4. Sporting / Hobby goods	13.9
	5. Consumer electronics (TV, VCR, cellular phones)	12.0
	6. Computer hardware or software	9.4
	7. Other	13.7
Shopping Frequency	1. More than once a week	20.3
	2. Once a week	22.5
	3. 2-3 times a month	34.4
	4. Once a month	12.1
	5. Less than once a month	10.7

Characteristics		Percentage
Knowledge about cookies (from somewhat to strongly agree)	1. I know a "cookie" is a small text file that a website's server places on my computer's web browser.	60.4
	2. I know the cookie transmits information back to the website's server about my browsing activities on the site, such as pages and content viewed, the time and duration of visits, search queries entered into search engines, and whether a computer user clicked on an advertisement.	49.2
	3. I know cookies also can be used to maintain data related to a particular individual, including passwords or items in an online shopping cart.	44.1
	4. I know some websites allow other third-party companies to place cookies into customers' hard drives to track shopping behaviors.	37.2

5.2 Preliminary Analysis

Before testing the measurement construct and structural model, assumptions for multivariate analysis, including multivariate normality and homocedasticity were examined. Kline (2005) suggests that there is a problem of multivariate normality when a Kurtosis value is greater than ten. The Kurtosis values in this study ranged from 1.95 to 2.55, indicating that the data did not have serious problems regarding data normality. Meanwhile, the skewness values (using a cut-off range from +1 to -1) also confirmed the normality of the data. Mplus version 6 (Muthen & Muthen, 1998-2010) software was used to analyze variance-covariance matrices. We used a two-step model-building approach including two conceptually distinct models: a measurement model and a path model (Kline, 2005). Missing data were estimated using Maximum Likelihood estimation, making it possible to use all available information in the dataset. Several model-fit indexes were used to assess confirmatory factor analysis (CFA) and structural equation model fit (SEM). Suggested by Hu & Bentler (1999), the Comparative Fit Index (CFI) $\geq$ .95, Non-Normed Fit Index (NNFI, also known as TLI) $\geq$ .95, Root Mean Square Error of Approximation (RMSEA) $\leq$ .06, and Standardized Root Mean Square Residual (SRMR) $\leq$ 0.08) were used to as cut-off lines in this study. Chi-square (χ^2) difference test was used to compare the model fit among models.

5.3 Measurement Model

The measurement model consisted of six latent constructs. Each latent construct was estimated by 3 indicators except the latent construct of perceived risk where two indicators were used to estimate perceived risk. A Confirmative Factor Analysis (CFA) was conducted and the one factor solution provided an excellent model fit, χ^2 ($_{df= 38}$) = 94.03, p <0.01, CFI=.99, TLI=.98,

RMSEA=.06, SRMR= .03. Standardized parameter estimates shown in Table 2 suggested the latent variables have been effectively measured by their respective indicators (factor loadings $>$.80). In addition, the standardized estimated error correlations between latent factors were checked by using .85 as the cutoff (Brown, 2006), which indicates that the measurement construct has good discriminant validity.

Structural Model

Following the CFA, the variance-covariance matrices were used to estimate the hypothesized structural model with Maximum Likelihood estimation. For exogenous variables, the number of third-party cookie identified in the scenario is coded as a continuous variable and the level of dissemination of consumer information was coded as a categorical variable (0=control, 1=share data internally, 2=share data both internally and externally). The proposed structural model (Figure 1) specified relationships among behavioral tracking, consumers' evaluations of online shopping experiences (perceived benefit, risk and unfairness), and their repurchase intentions.

The results of the SEM model suggested a good model fit, χ^2 (df= 55) = 126.36, p<.001, CFI = 0.98, TLI = .98, RMSEA = 0.06, SRMR = 0.04, demonstrating appropriate model fit for hypotheses testing (Hu & Bentler, 1999). Thus, no modification indices were used to respecify the model. Standardized parameter estimates (β) are shown in Figure 1.

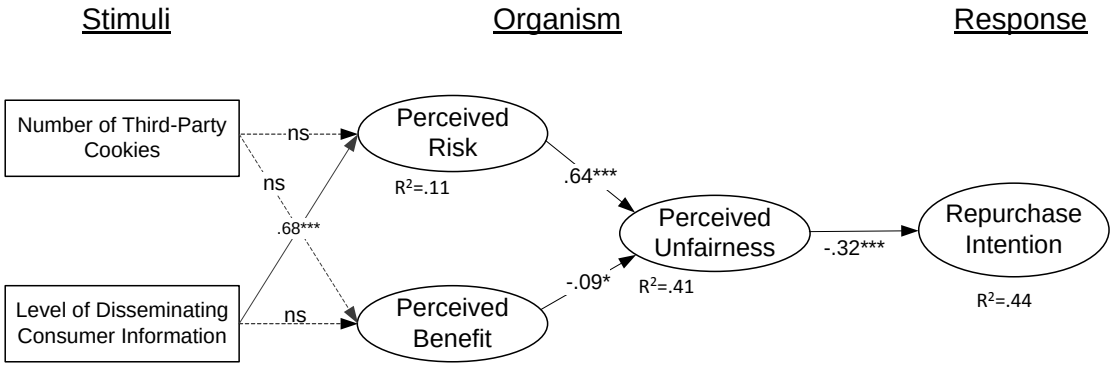

Figure 1 Structural model and hypotheses testing results. Note: All are standardized estimates. χ^2 (55) = 126.36, p < .001; CFI = .98; TLI= .98, RMSEA = .06; SRMR= .04, *p<.05, **p<.01, ***p<.001 (two-tailed); ns. non-significant.

Table 2. Confirmatory Factor Analysis and Measurement Model Results

Variable	Code	Items	Standardized Estimate	Estimate	SE	Critical Ratio	Cronbach's α
Perceived Risk (Pan & Zinkhan, 2006)	PR1	I think that buying a product from MyFavoriteStore.com would be risky because of the possibility of unauthorized access to my personal information.	.93	1.00	-	-	.91
	PR2	I think that buying a product from MyFavoriteStore.com would be risky because my personal information may be released to other third-parties.	.89	.93	.04	25.14	
Perceived Benefit (Revised from Yu & Cude, 2009)	BN1	I am pleased to see the advertisements of the brands I shopped when I use my social network website (e.g., facebook, myspace).	.86	1.00	-	-	.92
	BN2	I am pleased to see the personalized advertisements when I go to a news website (e.g., msn news, New York Times).	.91	1.05	.04	24.75	
	BN3	I am pleased to see the advertisements of the brands I shopped when I use online email services (e.g., Gmail, hotmail, yahoo! mail).	.91	1.04	.04	24.72	
Unfairness (Oliver and Swan, 1989)	PU1	I am pleased to see the personalized advertisements when I go to a news website (e.g., msn news, New York Times).	.88	1.00	-	-	.94
	PU2	I am pleased to see the advertisements of the brands I shopped when I use online email services (e.g., Gmail, hotmail, yahoo! mail).	.93	1.07	.03	32.00	
	PU3	Shopping on MyFavoriteStore.com is an unfair deal.	.93	1.04	.03	31.90	
Repurchase Intention (Chaudhuri and Ligas, 2009)	R1	I intend to return to shop at MyFavoriteStore.com.	.93	1.00			.93
	R2	I will use this store the next time I want to make a purchase.	.89	.93	.03	33.62	
	R3	I would recommend this store to my friends.	.90	1.01	.03	33.27	

Note. CFI = Comparative Fit Index; TLI = Tucker-Lewis index; RMSEA = Root Mean Square Error of Approximation; SRMR = Standardized Root Mean Square Residual; Goodness-of-Fit statistics: χ^2= 94.03 (*df* = 38, $p < .001$); CFI = .99, TLI = .98, RMSEA = .05, SRMR = .03.

Of the eight hypotheses proposed, four hypotheses were supported and one hypothesis was partially supported (Table 3). Hypotheses 1 to 4 tested the effect of behavioral tracking practices (the number of third-party cookies and dissemination level of consumer information) on consumers' perceptions of risk and benefit. Contrary to our predictions, the number of third-party cookies did not have significant effects on consumers' perceptions of risk or benefit. As a result, hypothesis 1 and 2 were not supported. The level of dissemination of consumer information had a significant effect on perceived risk (β =.68, p< .001) but not on perceived benefit (Hypothesis 4). Thus, only Hypothesis 3 was supported. Hypothesis 5 tested how perceived risk positively influences perceived unfairness of shopping on the websites. Hypothesis 5 was supported (β =.64, p< .001). Hypothesis 6 tested whether perceived benefit of personalized services negatively related to consumes' perceived unfairness of shopping on the websites. Hypothesis 6 was supported (β = -.09, p< .05). Hypothesis 7 tested whether the outcome of privacy calculus (perceived unfairness) significantly reduce consumes' repurchase intention of shopping on the websites. Hypothesis 7 was supported (β = -.32, p< .001). In order to evaluate the mediating effect of perceived risk, benefit and unfairness, the indirect effect of behavioral tracking practices on repurchase intention was examined. Results show the dissemination level of consumer information to have significant indirect effects on repurchase intention via perceived risk and unfairness with standardized estimates ranging from -.27 (t=-4.19, p>.001) to -.14(t=-.14, p<.001). Thus, Hypothesis 8 was partially supported. Standardized coefficients and unstandardized coefficients of direct effects and indirect effect from the behavioral practice on consumers' repurchase intention can be found in Table 4.

Table 3 Results of Hypothesis Testing

Hypothesis: Direct Effect Path	β		B	S.E.	C.R.	Results
H1: Third-party Cookie Amount→Perceived Risk	-.01		.00	.01	.56	N.S.
H2: Third-party Cookie Amount→Perceived Benefit	.06		.01	.02	.94	N.S.
H3: Disseminating Level→Perceived Risk	.68	***	1.07	.20	5.39	Supported
H4: Disseminating Level→Perceived Benefit	-.02		-.06	.18	.73	N.S.
H5: Perceived Risk→Unfairness	.64	***	.58	.04	13.56	Supported
H6: Perceived Benefit→Unfairness	-.09	***	-.09	.04	-2.03	Supported
H7: Unfairness→Repurchase Intention	-.32	***	-.36	.06	-5.51	Supported

Note: S.E.: Standard Error, C.R.: Critical Ratio.

Table 4 Direct, Indirect, and Total Effects of Level of Disseminating Consumer Information (Disseminating Level) on Repurchase Intention

Effects	*β*	B	S.E.	*C.R.*	*Sig.*
Direct	-.08	-.12	.18	-.70	n.s.
Total Indirect effects	-.41	-.66	.14	-4.89	***
Disseminating Level →Perceived Risk→ Repurchase Intention	-.27	-.43	.10	-4.19	***
Disseminating Level →Perceived Risk → Unfair → Repurchase Intention	-.14	-.22	.06	-3.77	***
Total effects	-.49	-.79	.20	-3.84	***

****p < .001, **p < .01, *p < .05.*

6. Discussion

The results offer several potential theoretical and practical implications within the apparel, shoe, and accessories industries. First, according to the significant result of Hypothesis 3, the study provides empirical evidence suggesting that young adults are concerned about their information privacy even when they are dealing with trusted online retailers. The present study provides evidence that consumers in this study care about whether their behavioral information will be broadly disseminated. Specifically, the level of dissemination of behavioral information significantly increases young consumers' perceived risk and perceived unfairness, influencing their evaluations of their online shopping experiences. In-line with prior research results, perceived risk is higher when consumers feel uninformed by marketers about how their information is collected and used (Lanier & Saini, 2008; Nowak & Phelps, 1995; Turow et al., 2009). However, contrary to our prediction, we did not find that the number of third-party cookies placed when visiting an online retailers' website had a significant effect on respondents' perceptions of risk and unfairness toward the online retailer. A possible explanation of this result may be the high cookie-deleting experience among the respondents (72.69%). It is speculated that respondents care less about tracking by third-party cookies because they may believe deleting cookies prevents their personal information from being collected and thus mitigates the privacy risk associated with third-party cookies. Alternatively consumers simply may not understand the magnitude of tracking and data sharing that is facilitated by third-party cookies.

Second, according to the significant result of Hypothesis 8, the effects of disseminating consumer information on respondents' attitudes toward online retailers are mediated by their perceptions of risk and unfairness. This is consistent with the findings in the literature that the influence of privacy concerns on consumers' behavioral intentions seems to be mediated by perceived unfairness of marketing strategies (Culnan & Bies, 2003; Malhotra et al., 2004). Thus, when consumers perceive that the behavioral tracking practices are risky and unfair, employing

behavioral tracking practices may hurt the long-term relationships between online shoppers and online retailers.

Overall, the findings suggest that consumers are concerned about their privacy with respect to the level of dissemination of their personal information for secondary uses by affiliates and third-parties, even when the data was shared by their trusted retailers. Findings are in-line with prior privacy research (Turow et al, 2009); however, the results of this study may more closely reflect the realities of online shopping situations than previous studies which did not account for the established relationship between consumers and retailers. Apparently, there is a disconnect between the privacy expectations of online shoppers and online retailers regarding what information should be collected from online shoppers and shared with others. Sharing of behavioral and demographic consumer information among affiliates and third-parties is fairly common in the online marketing industry despite the potential harm to customer relationships that such sharing may cause.

In turn, several practical implications of the study can be suggested. First, online retailers should be cautious about their information privacy practices related to behavioral tracking since they may lose consumers' trust if consumers perceive that these practices are unfair to them. As new techniques are developed to track and profile online consumers and to collect and share behavioral data for secondary usages such as providing personalized advertisements and products, consumers are less likely to be able to protect their own information privacy in the absence of clear notices and opportunities to do so. It is very important that online retailers provide clear, easy-to-understand explanations about their information practices that are at least accompanied by opt-out choices to enable consumers to knowledgeably participate in managing their online privacy. With regard to public policy makers, the present research provides empirical evidence about young-adult online shoppers' perceptions about online information privacy. Although the majority of respondents knew that cookie is a small text file that a website's server places on a computer's web browser, less than half knew that cookies transmit browsing activities information back to website servers and can be used to maintain data related to a particular individual. Furthermore, only 37.2 percent of respondents knew that some websites allow other third-party companies to place cookies into consumers' hard drives to track shopping behaviors. Findings suggest a need to improve consumers' privacy literacy.

Recently, federal legislation has been proposed to provide better privacy protection for consumers' personal information (Angwin, 2011). If enacted, such laws would likely regulate the information privacy practices of online retailers and other companies engaged in behavioral targeting (Angwin, 2011; King, 2011). It has been suggested that Congress should require companies to give consumers the right to decline to receive targeted advertising. Others suggest consumers should have a legal right to choose not to be tracked on websites that they visit, as

opposed to simply giving them a right to decline to receive targeted advertising (Angwin, 2011). Following the U.S. self-regulatory approach, industry associations have adopted privacy codes for their members that address behavioral targeting and consumer privacy (NAI, 2008; King, 2011). Additionally, the Digital Advertising Alliance (DAA) has created an icon for members to display in or near online advertisements or to post on web pages where data is collected and used for online behavioral advertising (FTC, 2012, p. 4). The icon relates only to online behavioral advertising involving third-parties, not contextual advertising that is based on the content of the web page being visited or a search query entered by the consumer. The DAAs icon alerts consumers about online advertising that is covered by a self-regulatory program. Clicking on the icon gives consumers access to a disclosure statement regarding the data collection and use practices associated with the ad as well as an opt-out mechanism (IAB, 2011). The FTC has recommended that the behavioral advertising industry offer consumers a "do not track" mechanism that works by placing a persistent setting, similar to a cookie, on a consumer's browser signaling the consumer's choices about being tracked and receiving targeted ads (FTC, 2010). Subsequently, Microsoft, Mozilla and Google announced plans to modify their Internet browsers to include "do not track" features that will enable users to limit online tracking (Bradley, 2011). Recently, controversy has arisen over whether the behavioral targeting industry will respect opt-out choices made by internet browsers that include default "do not track" features (BtoBonline.com, 2012). The effectiveness of opt-out ad icons and do not track browser features and the implications for the behavioral targeting industry of providing consumers with such controls are not yet known and may require more research.

7. Conclusion

As with any research, the results of this study should be interpreted in light of its limitations. First, the present study used manipulated scenarios as a forced exposure setting. Thus, the study ensured subjects were exposed to statements that provided notice of the online retailers' data dissemination practices and provision of third-party cookies, although it is recognized that many online shoppers may not actually notice this information in online retailers' privacy policies or understand the privacy implications of practices and technologies employed for data collection and data sharing. As a result, the use of manipulated scenarios in a forced exposure study may exaggerate the effect on consumers' perceptions of risk and unfairness regarding tracking practices of online retailers because information about online behavioral tracking technologies such as third-party cookies and related information privacy practices of online retailers is not so salient to consumers in the current online environment.

Second, the convenience sample of college students used in this study may constrain the ability to generalize the results of the study. However, at the same time, this study suggests that consumers' privacy concerns are context specific (FTC, 2009), and thus, the results of the

present study may better describe consumers' with specific characteristics, i.e., college students who shop for clothing, footwear, accessories, and books online.

The FTC(2012) stated that " [c]onsumers live in a world where information about their purchase behavior, online browsing habits and other online and offline activity is collected, analyzed, combined, used and shared, often instantaneously and invisibly" (p. i, Executive Summary). It has been shown that many online businesses do not promise or follow fair information practice principles in conducting their businesses (Earp, Anton, Aiman-Smith, & Stufflebeam, 2005; King, 2011; The Center for Democracy and Technology, 2009) and consumers can't opt-out of the behavioral tracking practices using the currently available mechanisms (Leon, Ur, Balebako, Cranor, Shay, & Wang, 2011). Amazon has been sued for knowingly using fake codes to communicate its privacy policy to Microsoft's Internet Explorer, leading the browser to accept the cookies that would otherwise have been blocked when consumers selected certain privacy settings (Internet Retailer, 2011)

We have several suggestions for future research based on the present research results. First, the majority of respondents in the present study (73%) reported that they had deleted cookies from their Internet browsers in the past. As a result, in future research, there is a need to interview consumers about why they delete cookies and whether they use other techniques to prevent online behavioral tracking such as using 'do not track' features in their Internet browsers. Second, the data exchanged and collected in different industries varied in extent and sensitivity. Future study can examine what personal data collected by apparel industry are sensitive to consumers. Third, future research might focus on how the chance to opt out of behavioral tracking practices impacts consumer behavioral responses of being tracked by marketers. Lastly, it is increasingly important to conduct studies that will empirically investigate mobile phone shoppers' privacy preferences. With the emergence of real-time location-based technologies and biometric identifiers that facilitate identification of individuals, combined with mobile marketing technologies directed at mobile phone users, the issue of behavioral tracking will continue to play a major role in debates about consumer privacy in the information age (King, 2008). In this era, ever increasing amounts of digital data are available to marketers and are an important resource for economic progress, but the granularity of the data available to marketers makes it increasingly difficult for consumers to protect their own privacy. As this topic become more prevalent, retailers will need to pay more attention to consumer information practices regarding data security and information privacy, as well as how their practices can enhance the consumer/retailer relationship.

Appendix A

Scenario Example

Your friend tells you to use a software program which helps you to identify whether third-party cookies are placed in your computer drive when you visit a website. After you used it, you find out that: YourFavoriteStore.com (where you frequently shop) **allow (0 or 14)** third-party cookies to be placed on your hard drive. However, YourFavoriteStore.com does **share** your personal information **with their corporate family** (and **companies outside of our corporate family**).

The website stated the following information in their privacy policy:

YourFavoriteStore.com **shares your personal information with our corporate family.**

(1) We may share information such as your name, postal and email address, customer preferences, and purchase history within our corporate family (affiliates - companies under common ownership) so that they may market to you. (2) When you visit our Website, we collect your navigational information, such as service-provider identification, IP address of your computer, the site that you navigate from, and the site that you navigate to when you leave. We may associate this navigational information with your personal information.

(The following statements were included in the condition of share consumer data externally)

YourFavoriteStore.com **also shares your personal information with companies outside of our corporate family.**

(1) We may also share your name, postal and email address, customer preferences, and purchase history with other merchants and merchant exchanges (non-affiliate companies that are not in our corporate family). (2) Other merchants may, in turn, use this information to send you offers about their products and services.

Bibliography

Angwin, J. (2011, August 10). Senators offer a privacy bill to protect personal data. *The Wall Street Journal.* Retrieved from http://online.wsj.com/article/SB10001424052748703385404576258942268540486.html

Bradley, T. (2011, February 10). Why browser 'Do Not Track' features won't work. *PCWorld*. Retrieved from: http://www.pcworld.com/printable/article/id,219328/printable.html

BtoBonline.com (2012, October 9). IAB urges members to ignore Microsoft's do not track default setting. *B2B Magazine*. Retrieved from: http://www.btobonline.com/article/20121009/DIRECT11/310099995/iab-urges-members-to-ignore-microsofts-do-not-track-default-setting

Brown, T. (2006). *Confirmatory factor analysis for applied research*. New York, NY: Guilford Press.

Chaudhuri, A., & Ligas, M. (2009). Consequences of value in retail markets. *Journal of Retailing, 85*(3), 406-419.

Chellappa, R. K., & Sin, R. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*, 181-202.

CNN. (2005). *Web sites change prices based on customers' habits*. Retrieved from http://articles.cnn.com/2005-06-24/justice/ramasastry.website.prices_1_price-differentials-price-discrimination-customers/3?_s=PM:LAW

Cranor, L. F. (1999). Internet privacy. *Communications of the ACM, 42*, 29–31.

comScore.com (2012, February 6). comScore reports $50 billion in Q4 2011 U.S. retail e-commerce spending, up 14 percent vs. year ago. Retrieved from http://www.comscore.com/Press_Events/Press_Releases/2012/2/comScore_Reports_Q4_2011_U.S._Retail_E-Commerce_Spending

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *The Journal of Social Issues, 59*(2), 323-342.

Dunfee, T. W., Smith, N., C., & Ross, W. T. (1999). Social contracts and marketing ethics. *The Journal of Marketing, 63*(3), 14-32

Earp, J. B., Anton, A., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management, 52*(2), 227-237.

Federal Trade Commission (FTC). (2007). *Fair information practice principles.* Retrieved from http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Federal Trade Commission (FTC). (2009). *FTC staff report: Self-regulatory principles for online behavioral advertising.* Retrieved from: www.ftc.gov/os/2009/02/P085400behavadreport.pdf

Federal Trade Commission (FTC). (2010). Protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers, Retrieved from: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

Federal Trade Commission (FTC). (2012). Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers, Retrieved from: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

Fox, S., & Madden, M. (2005). Pew internet and American life project, Retrieved from http://www.pewinternet.org/~/media/Files/Reports/2006/PIP_Generations_Memo.pdf.pdf

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing, 10*(Spring), 149-166.

Hawkins, D. I., Mothersbaugh D. L., & Best, R. J. (2007). Consumer Behavior: Building Marketing Strategy, McGraw-Hill/Irwin, New York

Huang, J. (2001). Consumer evaluations of unethical behaviors of websites: A cross-culture comparison. *Journal of International Consumer Marketing*, *13*(4), 51-71.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Model 6*(1), 1–55.

Interactive Advertising Bureau (2011). *Self-regulatory Program for Online Behavioral Advertising Factsheet*. Retrieved from: www.iab.net/media/file/OBA_OneSheet_Final.pdf

Ingram, R., Skinner, S., & Taylor, V. (2005). Consumers' evaluation of unethical marketing behaviors: The role of customer commitment. *Journal of Business Ethics, 62*(3), 237-252. doi:10.1007/s10551-005-1899-0.

Internet Retailer (2009[a]). *Top 500 guide: 2009 edtion.* Chicago: Vertical web media LLC.

Internet Retailer (2011). *Privacy suit takes aim at Amazon.* Retrieved from http://www.internetretailer.com/2011/03/04/privacy-suit-takes-aim-amazon

King, N. J. (2008). Direct Marketing, mobile phones, and consumer privacy: Ensuring adequate disclosure and consent mechanism for emerging mobile advertising practices, *Federal Communications Law Journal, 60*, 229-324.

King, N. J. (2011). Why privacy discussions about pervasive online customer profiling should focus on the expanding roles of third-parties. *International Journal of Private Law, 4*(2), 193-229.

Kline, R. B. (2005) *Principles and Practice of Structural Equation Modeling (2nd ed.).* New York, NY: The Guilford Press.

Lanier, C. D., & Saini, A. (2008). Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review, 12* (2), Retrieved from http://www.amsreview.org/articles/lanier02-2008.pdf

Larose, R., & Rifon, N. J. (2007). Promoting i-Safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs, 41*(1), 127-149.

Li, H., Sarathy, R. & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*, 434-445.

Leon, P. G., Ur, B., Balebako, R., Cranor, L. F., Shay, R., and Wang, Y. (2011, October 31). Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. Retrieved from http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Mayer, J. (2011) *Tracking the trackers: Where everybody knows your username.* Retrieved from http://cyberlaw.stanford.edu/node/6740

Mehrabian, A. & Russell, J. A. (1974). *An Approach to Environmental Psychology*, Cambridge, Mass.: MIT Press.

Milne, G. R., & Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing, 19*(2), 238-249.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing, 12*(2), 206-215.

Miyazaki, A. D. (2008). Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *Journal of Public Policy & Marketing, 27*(1), 19-33.

Network Advertising Initiative (NAI). (2008). 2008 NAI principles: The network advertising initiative's self-regulatory code of conduct, Retrieved from http://www.networkadvertising.org/pdfs/NAIComplianceRelease123009.pdf

National Retail Federation. (2007). Spending on dorm furnishings, electronics drives back-to-college sales past $31 Billion. Retrieved from http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=354

New York Times (2010) *Retargeting Ads Follow Surfers to Other Sites.* Retrieved from http://www.nytimes.com/2010/08/30/technology/30adstalk.html

Nowak, G., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when privacy matters. *Journal of Direct Marketing, 9*(3), 46–60.

Oliver, R. L., & Swan, J. E. (1989). Equity and disconfirmation perceptions as influence on merchant and product satisfaction. *Journal of Consumer Research, 16*, 372-83.

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing, 82*(4), 331-338.

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior, 28*(3), 1019-1027. doi: 10.1016/j.chb.2012.01.004

Pastore, M. (1999). Consumers will provide information for personalization. Retrieved from http://www.clickz.com/clickz/news/1717721/consumers-will-provide-information-personalization

Phelps, J., Nowak, G., & Ferrell. E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy &Marketing, 19*(Spring), 27–41.

Poddar, A., Mosteller, J., & Ellen, P. (2009). Consumers' rules of engagement in online information exchanges. *Journal of Consumer Affairs, 43*(3), 419-448.

Smith, H. J., Dinev, T. & Xu, H. (2011). Information Privacy Research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1015.

Stein, J. (2011). Data mining: How companies now know everything about you. *Time Magazine,* Retrieved from http://www.time.com/time/magazine/article/0,9171,2058205,00.html

The Center for Democracy & Technology. (2009). *Online behavioral advertising report.* Retrieved from: www.cdt.org/files/pdfs/CDT Online Behavioral Advertising Report.pdf

TRUSTe (2012). *Consumer privacy index-Q1*. Retrieved from http://www.truste.com/consumer-privacy-index-Q1-2012/

Turban, E., King, D., Lee, J., Liang, T., & Turban, D. (2010). *Electronic Commerce: A managerial Perspective*, Upper Saddle River, NJ: Prentice Hall.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., & Hennessy, M. (2009). Contrary to what marketers say, Americans reject tailored advertising and three activities that enable it (No. 025629-003). Retrieved from www.ftc.gov/bcp/workshops/privacyroundtables/Turow.pdf

Yu, J., & Cude, B. (2009). Hello, Mrs. Sarah Jones! We recommend this product! Consumers' perceptions about personalized advertising: comparisons across advertisements delivered via three different types of media. *International Journal of Consumer Studies, 33*(4), 503-514.